UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Items 1-3 as described in ATTACHMENT A

Case No. 21M610

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Items 1-3 as described in ATTACHMENT A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see attached affidavit and ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United States Code, Sections 1708, 514(a), 1028A, 1029, and 371.	Mail Theft (18 USC 1708), Fictitious Obligations (18 USC 514(a)), Aggravated Identity Theft (18 USC 1028A), Access Device Fraud (18 USC 1029), and Conspiracy (18 USC 371)

The application is based on these facts:

See attached affidavit and ATTACHMENTS A and B.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

@ 12:47PM
Applicant's signature

MATT SCHMITZ, U.S. POSTAL INSPECTOR
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ *(specify reliable electronic means).*

Date: 1-21-2021

Judge's signature

City and state: Green Bay, WI

U.S. Magistrate Judge James R. Sickel
Printed name and title

AFFIDAVIT

I, Matthew Schmitz, United States Postal Inspector, being duly sworn, state the following information was developed from the Affiant's personal knowledge and from information furnished to the Affiant by other law enforcement agents and business contacts:

I. INTRODUCTION

1. I have been a Postal Inspector with the United States Postal Inspection Service for approximately 16 years and am currently assigned to the Green Bay (WI) Domicile in the Eastern District of Wisconsin. Before becoming a Postal Inspector I served as a police officer with the Janesville Police Department in Janesville, Wisconsin for one year and as a police officer and detective with the Middleton Police Department in Middleton, Wisconsin for approximately five years. As a Postal Inspector I am responsible for investigating criminal violations that involve the United States Mail and United States Postal Service. These investigations include, but are not limited to, mail fraud, mail theft, credit card fraud, identity theft, personal and business check forgeries, controlled substance distribution, burglaries and robberies of United States Postal Service facilities and its employees, and conspiracies regarding those offenses. I have conducted mail theft investigations that have also involved the theft of gift cards, credit cards, personal and business checks, debit cards, and personal identifying information (PII) contained within those stolen mailings.

PURPOSE

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—described in Attachment A—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. The property to be searched as identified in ATTACHMENT A is currently in the possession of the U.S. Postal Inspection Service in Oneida, WI, and the De Pere (WI) Police Department. Therefore, all property to be searched as listed in ATTACHMENT A is currently located in the Eastern District of Wisconsin. This warrant

would authorize the forensic examination of the property listed in ATTACHMENT A for the purpose of identifying electronically stored data particularly described in ATTACHMENT B.

DEFINITIONS

4. Based on my training and experience, I use the following technical terms to convey the following meanings:

   a. Cellular Telephone or Cellular Devices: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

   b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

   c. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

COMPUTERS AND ELECTRONIC STORAGE

5. This warrant seeks the Court's permission to search and seize records as identified in ATTACHMENT B that might be found on the property identified in ATTACHMENT A, in whatever form it is found. I submit that there is probable cause to believe the evidence described in ATTACHMENT B will be stored on the property identified in ATTACHMENT B based upon the facts provided in this affidavit and for the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Similarly, files that have been viewed via the Internet are typically automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

6. I know from my training and investigative experience that when an individual uses a computer to produce counterfeit documents, checks, identification cards, and other instrumentalities in furtherance of the scheme, that computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

FACTS

7. On November 12, 2020, at approximately 6:00 PM, the De Pere (WI) Police Department made contact with a male later identified as Hue Lor at the Community First Credit Union (CFCU) at 1700 Lawrence Drive in De Pere, WI regarding a check fraud investigation. CFCU staff had contacted the De Pere Police to report an Asian male (later identified as Hue Lor) was at their financial institution trying to cash a fraudulent check. CFCU said Lor presented two (2) checks that were altered with a different payee name and dollar amount.

8. De Pere Police Officer Lee Townsend arrived at CFCU on November 12, 2020, and saw an Acura MDX SUV with Wisconsin registration ACH3929 was parked near the front door of the credit union. Officer Townsend entered the credit union and made contact with Lor who he initially identified as "Saman Homesombath" based on identification cards Lor presented. Officer Townsend noticed the photograph on

the ID card Lor presented in the name of Saman Homesombath was not the same individual he was speaking with. Officer Townsend reported Wisconsin Department of Transportation (DOT) records identified the Acura MDX SUV with Wisconsin registration ACH3929 had been sold to Hue Lor in October, 2020. Officer Townsend identified Lor's personal identifying information and photograph and verified the individual he was in contact with at the CFCU was Hue W Lor, M/A, 11/21/1986. You affiant believes Lor utilized this vehicle to travel to the CFCU considering Lor was the only customer inside the bank when officers made contact with him, the Acura MDX with WI registration ACH3929 was the only vehicle parked in the customer parking area near the bank's entrance, and WI DOT records reported this vehicle had been sold to its new owner, Hue Lor, in October, 2020.

9. On November 18, 2020, De Pere Police Detective Sergeant (Det/Sgt) Steve Yedica executed a search warrant on the 2004 Acura MDX with Wisconsin registration ACH3929. This warrant was approved by Brown County Circuit Court Commissioner Paul Burke earlier that same day. Det/Sgt Yedica located and seized the following items (summary list):

a. Numerous blank checks drawn on the accounts of different individuals.

b. Blank check stock.

c. Personal and business checks payable to numerous individuals, including Hue Lor, that appeared to have had the payee and dollar amount information altered.

d. Numerous debit, credit, and gift cards.

e. Numerous pieces of opened US Mail 1st Class letters containing different sender and addressee names. Further examination of these letters shows they appear to have been mailed by individuals in Wisconsin to other individuals and businesses.

f. Numerous identification cards in different names.

g. Suspected methamphetamine and paraphernalia associated with methamphetamine use.

h. Electronic storage devices, computers, scanner/printer, and cell phones (see below).

i. Nail polish remover and a sponge that appeared to have been used to remove ink from checks.

10. As documented in item h of paragraph 9 of this affidavit, Det/Sgt Steve Yedica seized electronic storage devices, computers, scanner/printer, and cell phones. In particular, those items are further identified as:

a. An LG brand cellular telephone with model number LM-Q730TM and serial number 35490111724276.

b. A black Micro USB portable electronic storage device.

c. A black Samsung tablet model SM-T560NV and serial number R52M104ELXL.

d. A Western Digital 640GB external hard drive with model number WD6400AAKS and serial number WMA8Y4626493.

e. A Seagate 500GB hard drive with serial number W62HC33L.

f. A Hitachi 750GB hard drive with serial number 59G1L7LE.

g. An Hp laptop computer model 15-dw1083wm with serial number CND0425V16.

h. A Toshiba 500GB external hard drive with model number DTC805 and serial number 9571THMMTTK8.

i. A Canon Pixma model K10483 printer/scanner with serial number KMPC50827.

j. An Hp LaserJet Pro MFPM29w printer/scanner with serial number VNB3S86580.

k. An Hp Chromebook model 14-SMB with serial number 5CD4181RMR.

l. A black Alcatel Android cellular device with IMEI number 015500002272732.

m. A Gateway model MD2614u laptop computer with serial number LXW790X0049010403A2600.

n. A Hp Pavilion computer tower with model number s5704y and serial number 3CR047037W.

11. I examined photographs Det./Sgt. Yedica had taken of the evidence he seized from Lor's Acura MDX. In particular, I saw the Hp LaserJet Pro printer/scanner identified in paragraph 10 item j contained a sheet of check stock under its lid. This sheet of check stock contained three checks all purporting to be payable from "Apricity, 1010 Strohmeyer Dr, Neenah, WI 54956" to "Sherman Lee Thao" (2 checks) and "Saman Homesombath."

12. On November 13, 2020, as a result of the investigation by De Pere Police regarding Hue Lor's conduct at the CFCU, Lor was charged in Brown County Circuit Court under case number 2020CF001785 with misappropriating personal identifying information, forgery, and resisting/obstructing an officer. On November 22, 2020, Hue Lor took custody of his vehicle, the 2004 Acura MDX with Wisconsin registration ACH3929, from the De Pere Police Department. The property identified above in paragraphs 9 and 10 has been retained as evidence by the De Pere Police Department.

13. During the course of this investigation Inspector Schmitz learned from Det/Sgt Yedica that a counterfeit check drawn on the Associated Bank account of Wayne and Lynn Wayrynen of Appleton, WI had been cashed at the Ashwaubenon branch of Associated Bank in the amount of $1,100. This incident occurred on November 10, 2020. Associated Bank had provided images of the counterfeit check that was presented (check #15015) along with surveillance photographs taken at the drive-through lane of Associated Bank where the check was presented. I (Inspector Schmitz) saw check #15015 drawn on the Associated Bank account of Wayne and Lynn Wayrynen had been made payable to "Saman Homesombath." Further, Associated Bank surveillance photos showed the individual presenting the check through their drive-through was an Asian male driving an Acura with Wisconsin registration ACH3929.

14. Inspector Schmitz contacted Lynn Wayrynen during the course of this investigation and learned from her that she and her husband, Wayne, had a checking account at Associated Bank that had recently been victimized through counterfeit checks. Lynn said they had never made a check on their Associated Bank account payable to "Saman Homesombath" and, as of December 11, 2020, still had check number 15015 in their checkbook. Lynn said she did not know how her account had been compromised, but recalled she had mailed check numbers 14995 and 14994 in her mailbox on or about November 8, 2020, to pay two different bills.

15. On December 9, 2020, Stevens Point (WI) Police Detective John Lawrynk contacted me to report that the Stevens Point Police Department had engaged in a vehicle pursuit involving Hue Lor's 2004 Acura MDX with Wisconsin registration ACH3929 earlier that morning. Lor was a passenger in the vehicle while the driver was identified as Joseph Thammavongsa. Following the pursuit Lor's vehicle was impounded at the Stevens Point Police Department.

16. Portage County drug investigators had developed information in the past showing Thammavongsa was suspected of being a methamphetamine distributor and user. In consultation with the Portage County District Attorney's Office, Stevens Point Police executed a certified drug K-9 examination of the exterior of Lor's vehicle while it was at the Stevens Point Police Department and a subsequent search of this vehicle. Stevens Point Police K-9 Officer Austin Lee reported his certified drug detection dog alerted to the odor of controlled substances while the dog walked around the vehicle. Based upon the K-9 alert, Officer Lee, Detective John Lawrynk, and Assistant Chief Bob Kussow searched the interior of Lor's 2004 Acura MDX and seized:

a. A methamphetamine pipe, a digital scale and two small gem baggies both which had white powdery residue.

b. Numerous identification cards in the names of people other than Hue Lor and Joseph Thammavongsa.

c. Numerous pieces of US Mail letters containing different sender and addressee names. Further examination of these letters shows they appear to have been mailed by individuals in Wisconsin to other individuals and businesses.

d. Packages of blank check stock.

e. Computers, an electronic storage device, cell phones, and a printer (see below).

f. Photocopies of identification cards with the same photograph but different names and dates of birth.

g. Numerous debit and credit cards under the names of different individuals.

h. Numerous checks payable to different individuals.

i. A copy of the Brown County search warrant of Lor's vehicle executed in November, 2020, by De Pere Det/Sgt Steve Yedica.

17. During the course of this investigation Det. Lawrynk told me that the Wisconsin State Patrol arrested Blong Vang in the Stevens Point, WI area after he was found to be driving a car that had been stolen. Det. Lawrynk contacted the stolen vehicle's owner and obtained consent to search the vehicle. He executed this search on December 14, 2020, and found it contained the below items. I took custody of these items from Det. Lawrynk on December 15, 2020, and currently have them secured at the U.S. Postal Inspection Service office in Oneida, WI, in the Eastern District of Wisconsin.

a. Identification cards in the names of other people.

b. Handwritten notes displaying various email addresses, passwords, bank account information, and suspected credit/debit account information.

c. Various paperwork in the name of Blong Vang.

d. A Visa debit card, US Mail envelopes, US Bank statement, BMO Harris bank mailing, Fox Communities Credit Union mailing, and 2018 Wisconsin State Income Tax form all in the name of Hue Lor.

e. A black MicroSD card.

f. A black Samsung Galaxy G7 cellular device.

g. A blue Nokia Cricket cellular device.

18. I believe the items found in the stolen vehicle Blong Vang was driving are indicative of his involvement in this investigation that includes Hue Lor and Joseph Thammavongsa, among others both known and unknown at this time. Specifically, based upon my training and investigative experience I have learned that individuals involved in mail theft, identity theft, check fraud, and debit and credit card fraud, commonly possesses and retain the identification and personal identifying information of others to be able to use that information at a later date to obtain fraudulent credit and debit accounts and produce counterfeit checks. Furthermore, I have learned that these individuals also commonly use electronic devices such as computers, cellular telephones, and portable electronic storage devices to assist them in their mail theft and fraud schemes. Computers, cellular devices, and portable electronic storage devices can all be used to store personal identifying information and can be used as a tool in reproducing documents, checks, and

identification cards as well as submitting fraudulent applications to financial institutions for credit and other accounts. For these reasons and based upon the facts submitted in this affidavit, I believe the Blong Vang is involved in a mail theft and/or fraud scheme with Hue Lor and others, and has used the black MicroSD card, black Samsung Galaxy G7 cellular device, and the blue Nokia Cricket cellular device identified in paragraph 17 in furtherance of this theft and fraud scheme.

19. During the course of this investigation I have reviewed investigative reports and photographs of evidence related to the investigations conducted by Det/Sgt Yedica and Det. Lawrynk. I determined from those reports and the evidence seized that the individuals involved in this scheme appear to be stealing and opening U.S. Mail to obtain checks, credit cards, debit cards, and PII. In particular, checks that are stolen from the mail are later reproduced or "washed" so that new information (payee, dollar amount, check date) can be written or printed on the check and later cashed by others. I am aware from my training and investigative experience that mail theft schemes targeting mailings that likely contain personal or business checks commonly use the stolen check/s to reproduce counterfeit checks or to remove the existing payment information through "washing," a process in which household chemicals are used to lift or erase the ink on a check and then, once dried, write new information on the check. Further, based upon my training, investigative experience, and the facts presented in this affidavit, I believe Hue Lor and others are using proceeds they obtain from stealing mail and forging and counterfeiting checks and credit contained within that stolen mail to purchase methamphetamine. I believe this is true for several reasons including, (1) suspected methamphetamine and associated paraphernalia was found in Hue Lor's vehicle on two occasions in November, 2020, and December, 2020, by De Pere Police and Stevens Point Police, respectively, (2) both Hue Lor and Joseph Thammavongsa have arrests in 2020 for possession of methamphetamine (Lor) and manufacture/deliver amphetamine (Thammavongsa), and, (3) I have learned through my training and investigative experience as a Postal Inspector that some methamphetamine users participate in mail theft, and check and credit card fraud to fund their purchases of methamphetamine.

20. Further, based upon my training, investigative experience and the facts presented in this affidavit, I believe probable cause exists that the electronic devices identified in ATTACHMENT A and paragraph 17 of this affidavit were used in furtherance of this scheme. I have learned from my training and investigative experience that:

a. Individuals engaged in mail theft, check counterfeiting and fraud, and credit card fraud and identity theft typically use computers and printers to create the counterfeit checks and IDs and print them out on blank check stock or blank IDs. Further, individuals engaged in credit card fraud and using PII to obtain credit cards and other lines of credit in the names of others must use a computer or electronic device that has access to the internet in order to complete the application in support of the fraudulent account.

b. Individuals engaged in mail theft, check counterfeiting, and credit card fraud commonly use hard drives or portable electronic storage devices in furtherance of their scheme to defraud. Such devices allow their users to store large amounts of data including pictures, video, and other information. Individuals involved in producing counterfeit checks and/or obtaining fraudulent credit accounts require a computer or other electronic storage device in order to retain images and data of the checks they are producing and printing or the accounts they have fraudulently applied for.

c. Individuals engaged in mail theft, check counterfeiting, and credit card fraud typically use phones to communicate with others involved in the scheme via telephone calls, text records, and/or social media account communication, and/or take photographs of checks, identification cards, stolen US Mail, other individuals and/or victims, or personal identifying information. Further, because many modern cellular devices act similarly to a computer and can access the internet, these devices may contain internet search information related to credit card fraud and/or check fraud. Also, when using a cellular signal, cellular devices communicate with cell towers. Those towers are fixed to a particular location and the cellular device using that particular tower makes a record of that particular tower's use. Most individuals retain possession of their cellular device wherever they travel. This is also especially true with individuals involved in mail

theft, check fraud, and credit card as having immediate access to a device that allows them to instantly communicate with others involved in the scheme is crucial to the success of the scheme. Accessing location data on a cellular phone associated to an individual involved in a mail theft, check fraud, and credit card fraud scheme can provide evidence of where mail theft, check fraud, and credit card fraud may have occurred.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that the devices described in ATTACHMENT A can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. As further described in ATTACHMENT B, this application seeks permission to locate electronically stored information that might serve as direct evidence of the crimes described on the warrant. Such evidence will consist of calling logs, contact list information, text message information, images and photographs, IP logs, documents, spreadsheets, and internet query information that relate to the use of the property to communicate with others, including co-conspirators and Hue Lor, or to gather (stolen US Mail), reproduce, or distribute counterfeit checks, negotiable monetary instruments, identification cards, credit cards, debit cards and PII. This evidence will also establish how the property was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion on to a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. Based on the facts set forth in this affidavit, I believe probable cause exists to show that the devices described in ATTACHMENT A contain the items listed in ATTACHMENT B of this affidavit. Therefore I am seeking the issuance of a warrant to search the devices for the items described in ATTACHMENT B, in

violation of 18 USC 1708, Mail Theft, 18 USC 514(a) Fictitious Obligations, 18 USC 1028A, Aggravated ID Theft, 18 USC 1029, Access Device Fraud, and 18 USC 371, Conspiracy.

12:47PM

Matthew B. Schmitz
U.S. Postal Inspector

Subscribed and sworn to before me this 21 day of January, 2021.

The Honorable James R. Sickel
United States Magistrate Judge
Eastern District of Wisconsin

ATTACHMENT A: PROPERTY TO BE SEARCHED

1. A black MicroSD card.
2. A black Samsung Galaxy G7 cellular device.
3. A blue Nokia Cricket cellular device.

These Devices are currently all located in the Eastern District of Wisconsin and in the possession of the U.S. Postal Inspection Service Green Bay Domicile in Oneida, WI. This warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

ATTACHMENT B: PARTICULAR THINGS TO BE SEIZED

1. All records on the Devices described in Attachment A that relate to violations of 18 USC 1708, Mail Theft, 18 USC 514(a) Fictitious Obligations, 18 USC 1028, Aggravated ID Theft, 18 USC 1029, Access Device Fraud, and 18 USC 371, Conspiracy, since August 1, 2020, including:

   a. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

   b. Call log history.

   c. Address book or contacts lists.

   d. Records of internet search activity including records involving the search or query of files related to the location of banks, "washing" counterfeit checks, producing counterfeit checks, applying for credit cards, loans, or lines of credit, producing identification cards, and mail theft.

   e. Records identifying any text messages or text message history.

   f. Records identifying the historical location of the Devices.

   g. Photographs or images depicting what is believed to be US Mail, checks, credit cards, banks, applications for credit cards, loans, or lines of credit, identification card information (an individual's face and/or PII), personal identifying information (PII), controlled substances and paraphernalia related to the use of controlled substances, and US Currency.

   h. Ledgers, logs, or spreadsheets.

   i. Records discussing mail theft, check fraud, credit card fraud, and controlled substance use.

2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.